HCI International 2024
29 June - 4 July 2024
Washington Hilton Hotel, Washington DC, USA

Call for Participation
Burnout in the Cybersecurity Profession – What, Why, How

Saturday June 29, 8:30 AM – 12:30 PM

Organizer(s):

Dr. Calvin Nobles
University of Maryland Global Campus, Adelphi, MD, USA
calvin.nobles@umgc.edu

Dr. Ann Rangarajan
Illinois Institute of Technology, Chicago, IL, USA
arangarajan@iit.edu

Dr. Benjamin Yankson
University at Albany, State University of New York, Albany, NY, USA
byankson@albany.edu

Vatsla Gupta
Illinois Institute of Technology, Chicago, IL, USA
vgupta32@hawk.iit.edu

Aim of the workshop

Cybersecurity is more than a technological endeavor; it is a socio-technical problem involving complex interactions among humans, organizations, social, economic, and technical factors requiring engagement across all societal sectors (National Science and Technology Council, 2019). One such challenge is the phenomenon of burnout among cybersecurity professionals.

Burnout amongst cybersecurity professionals is increasingly acknowledged in both industry settings and academic literature (Budge et al., 2023; Nobles, 2022; Platsis, 2019; Reeves et al., 2023). The World Health Organization has classified burnout as an occupation-related syndrome (World Health Organization, 2019) that can result in an increased error rate, leading to cybersecurity risk with significant associated and financial or reputational impact on the organization. Notwithstanding this risk, it increases employee turnover, decreases productivity, excessive stress, decreases motivation, and increases fatigue. We aim to examine this nascent topic with a socio-technical lens to gain a deeper understanding of the problem and develop early-stage interventions at individual, organizational, and societal levels.

Expected workshop outcome

1. We expect that the workshop will bring together a rich cohort of interdisciplinary academics and industry professionals with an interest and passion in the cybersecurity field, drawing from cybersecurity engineering and operations professionals, cybersecurity leadership (e.g. Chief Information Security Officers, Business Information Security Officers), cyber risk analysts, behavioral psychologists, and human factors engineering experts. By bringing together such a wide variety of experts from different domains, the event will initiate exciting interdisciplinary collaborations that could lead to future large-scale collaborative projects on the topic of burnout

2. An outcome of the workshop will be to sharpen our understanding of the main challenges and problems in this domain and lay down a foundational roadmap for joint academy-industry collaborative research in this area

3. We anticipate that the workshop will serve to strengthen the identity of an emergent multi-disciplinary research community whose common goal is to develop socio-technical solutions to emerging technological challenges in cybersecurity

Workshop topics

We welcome practitioners and researchers in the field of Cybersecurity to participate in a collaborative session to discuss and professionally debate a breadth of questions including the following.

I. Antecedents of burnout	**II. Manifestation of burnout**
● What are the causes of burnout in cybersecurity? ● How does organizational culture within the cybersecurity industry influence the development and management of burnout? ● How do the stressors unique to cybersecurity, such as the persistent threat environment and the rapid pace of technological change, exacerbate the risk of burnout?	● How do cybersecurity professionals recognize or identify the onset of burnout? ● How do signs of burnout manifest at the individual contributor, mid-level manager, and senior leader levels?
III. Impact & prevention of burnout	**IV. State-of-the-art academic literature on burnout**
● How do cybersecurity professionals deal with burnout today? ● What are the impacts of burnout at an individual level? ● What are the impacts of burnout at an organizational level? ● What preventative strategies effectively reduce the risk or impact of burnout among cybersecurity professionals?	● What definitions of burnout have been used in cybersecurity literature? ● What interventions and organizational policies have been discussed or implemented to mitigate burnout among cybersecurity workers, and with what success? ● What gaps exist in the current literature regarding burnout in cybersecurity, and what areas require further empirical research?

Workshop agenda

The following is a framework for the program of the workshop:

Time	***Program event***
8:30 – 8:45	Introduction & Workshop Logistics
8:45 – 9:30	Topic I discussion: **Antecedents of burnout**
9:30 – 9:40	Topic I re-cap & wrap-up
9:40 – 10:20	Topic II discussion: **manifestation of burnout**
10:20 – 10:30	Topic II re-cap & wrap-up
10:30 – 11:00	Refreshment Break
11:00 – 11:45	Topic III discussion: **Impact and prevention of burnout**
11:45 – 11:55	Topic III re-cap & wrap-up
11:55 – 12:05	Topic IV discussion: **state-of-the-art academic literature on burnout**
12:05 – 12:15	Topic IV re-cap & wrap-up
12:15 – 12:30	Workshop wrap-up, next steps

Guidelines to prospective authors

Submission for the Workshop

Prospective authors should submit their proposals in PDF format through the HCII Conference Management System (CMS). You are welcome to submit your ideas exploring the workshop topics in the form of short papers, research in progress whitepapers, and abstracts.

Submission for the Conference Proceedings

The contributions to be presented in the context of Workshops will not be automatically included in the Conference proceedings.

However, after consultation with the Workshop Organizer(s), authors of accepted workshop proposals that are registered for the conference are welcome to submit, through the HCII Conference Management System (CMS), an extended version of their workshop contribution to be considered, following further peer review, for presentation at the Conference and inclusion in the "Late Breaking Work" conference proceedings, either in the LNCS as a long paper (typically 12 pages, but no less than 10 and no more than 20 pages), or in the CCIS as a short paper (typically 6 pages, but no less than 4 and no more than 8). The submission deadline for the camera-ready papers (long or short) for the "Late Breaking Work" Volumes of the Proceedings is the 24th of May 2024.

Workshop deadlines

Submission of workshop contributions	30 April 2024
Authors notified of decisions on acceptance	10 May 2024
Finalization of workshop organization and registration of participants	10 May 2024

Workshop organizer(s)

Dr. Calvin Nobles

Dean and Portfolio Vice President, School of Cybersecurity and Information Technology at University of Maryland Global Campus (UMGC)
https://www.linkedin.com/in/calvinnobles/

Dr. Calvin Nobles' scholarly pursuits are situated at the nexus of human factors engineering and cybersecurity. His research elucidates the multifaceted impacts of security fatigue, burnout, stress, and distractions on system integrity and personnel well-being. Additionally, Dr. Nobles examines the dynamics of human performance and behavioral patterns, focusing on the incidence and management of human errors. His work advocates for integrating comprehensive human factors programs within cybersecurity frameworks, utilizing human factors analysis and classification systems as tools to dissect, alleviate, and preempt error occurrence. He seeks to optimize the relationship between users and digital mediums, using the lens of human-computer interaction and advanced human factors engineering, thereby minimizing the friction encountered in utilizing digital interfaces and devices.

Dr. Ann Rangarajan

Assistant Professor, Department of Information Technology and Management, Illinois Institute of Technology, Chicago IL
https://itm.iit.edu/rangarajan/

Dr. Ann Rangarajan's research is guided by an overarching framework that holistically examines individual, organizational, societal, and cultural factors underlying complex socio-technical systems that impact technology management. Her interdisciplinary research interests lie at the intersection of applied computer science and computer systems engineering, information systems (IS) innovation and diffusion, and socio-technical factors impacting technology implementations. Before entering academia, Ann worked for global Fortune 100 organizations in a broad range of Information Technology and Information Systems leadership roles for twenty-five years. In addition, she brings over twelve years of teaching experience across Information Systems and Information Technology curriculum in the College of Technology, School of Business, and School of Information Sciences at reputed higher education institutions.

Dr. Benjamin Yankson

Graduate Director, Cybersecurity / Assistant Professor, College of Emergency Preparedness, Homeland Security, and Cybersecurity (CEHC) University at Albany, State University of New York, Albany, NY
https://www.albany.edu/cehc/faculty/benjamin-yankson

Dr. Yankson is currently an Assistant Professor and a Graduate Program Director in the Department of Cybersecurity at the University at Albany, SUNY. His research touches many vibrant and exciting areas in Cybersecurity, Privacy, Information Science, and Complex systems. Dr. Yankson focuses on Privacy and Security of Small Scale IoT security for vulnerable populations (Children's Smart Toys), Operational Security (OPSEC) risk, Digital Forensics, Cybersecurity Compliance, and Cybersecurity Capacity building. He conducts technical and interdisciplinary research that uses mixed methods to address complex Privacy and Cybersecurity problems. Dr. Yankson is the Director of CEHC HackIoT Lab, and founder of Global CyberTech Exchange. He spent over 15 years in the Information Technology and Cybersecurity industry and held various technical and leadership roles.

Vatsla Gupta

MBA student at Illinois Institute of Technology, Chicago IL
https://www.linkedin.com/in/vatsla-gupta-mba-cisa-ceh-a5210a1b/

Miss Vatsla Gupta is a MBA student at the Illinois Institute of Technology, boasting a decade of comprehensive experience of more than nine years in the realms of Security and Compliance. Her expertise extends across diverse areas, including proficiency in tools like Splunk Cloud, extensive experience in logging and auditing various information systems, and a proactive approach to system security through the CIA triad methodology. Notably, she has actively contributed to ensuring compliance with PCI DSS (Payment Card Industry Data Security Standard) and has served as a SOC (Security Operations Center) Analyst, showcasing her proficiency in managing and enhancing security measures in line with industry standards.

Registration regulation

Workshops will run as 'hybrid' events. Participants will have the option to attend either in-person or virtually. The total number of participants per workshop cannot be less than 8 or exceed 25.

Workshops are ‘closed’ events, i.e. only authors of accepted workshop proposals, registered for the specific workshop, will be able to attend.

Registration for workshops is complimentary for registered conference participants.

Useful links and References

Budge, J., Roberts, J., Shey, H., & Levine, D. (2023, February 14). *We need to talk more about burnout in Cybersecurity*. Forrester. https://www.forrester.com/blogs/we-need-to-talk-more-about-burnout-in-cybersecurity/

National Science and Technology Council (US). Interagency Working Group on Cyber Security and Information Assurance. (2019). *Federal Cybersecurity Research and Development Strategic Plan*. Executive Office of the President of the United States.

Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. *HOLISTICA–Journal of Business and Public Administration*, *13*(1), 49-72.

Platsis, G. (2019, August 14). Is staff burnout the best reason to implement cybersecurity A.I.? Securityintelligence.com. Retrieved from https://securityintelligence.com/articles/is-staff-burnout-the-best-reason-to-implement-cybersecurity-ai/

Reeves, A., Pattinson, M., & Butavicius, M. (2023, July). Is Your CISO Burnt Out yet? Examining Demographic Differences in Workplace Burnout Amongst Cyber Security Professionals. In *International Symposium on Human Aspects of Information Security and Assurance* (pp. 225-236). Cham: Springer Nature Switzerland.

World Health Organization. (2019). QD85 Burnout. In International statistical classification of diseases and related health problems (11th ed.). https://icd.who.int/browse11/l-m/en#/http://id.who.int/icd/entity/129180281